A Nation Under Civic Digital Stress and One Standardized Rider That Could Help Tie the States Together

Non-Agentic CROSS-STATE CIVIC DIGITAL VISIBILITY RIDER Initiative

(Legislative Proposal Inspired by Benjamin Franklin's Creation of the American Postal System)

Christopher Hunt Robertson, M.Ed.
with Collaborative Support from Perplexity and ChatGPT

To their credit, our state legislatures are working to protect our civic institutions from escalating digital attacks. They are responding in visible, earnest, and highly uneven ways: with cyber units, continuity planning, vendor rules, court modernization, AI bills, hospital reforms, and local-government resilience proposals. But the response remains fragmented. Each state sees the injury closest to hand and proposes a remedy fitted to that one domain. The result is not apathy, but patchwork. What's missing from their legislative efforts is a modest, standardized attachment - a rider - that could travel across these otherwise different bills and quietly connect them. The rider I'm proposing is the ***Cross-State Civic Digital Visibility Rider.*** This mechanism would allow states to coordinate AI safety and digital infrastructure governance completely independent of federal action. By embedding identical, standardized rider language into local state-level bills, states could form an adaptive, cross-state network of data sharing. This would create an aligned framework for managing technology risks without needing a gridlocked federal Congress to pass comprehensive national legislation.

(Image by ChatGPT)

In 1775, Benjamin Franklin was not trying to persuade thirteen colonies to become identical. He was trying to persuade them to share a practical civic infrastructure: a postal system with common routes, standards, and expectations that could bind scattered communities into a functioning public sphere.

The United States now faces a similarly practical problem in digital form. Costly civic digital attacks are no longer speculative or regional; they are well documented in every state - across hospitals, courts, airports, legislatures, tax agencies, schools, public housing authorities, and municipal networks. Proposed here is a new approach to that growing problem:

***Cross-State Civic Digital Visibility Rider* Proposed for All Civic AI - Related Legislation in Participating States:**

"Any digital system, automated tool, or networked service governed by this Act shall include Non-Agentic Civic AI visibility mechanisms that inform elected officials and the public about material digital risks affecting covered public entities, while preserving meaningful human decision-making and constitutional authority. These mechanisms may include public, privacy-respecting summaries of where critical data and dependencies reside, high-level reporting on significant incidents and remediation progress, and anonymized statistics on recurring vulnerabilities. They shall not make recommendations, take actions, or exercise governmental authority."

The argument is simple. First, costly civic digital harm is now clearly documented in every state. Second, states are struggling to respond through a mixed and reactive body of legislation. Third, a standardized rider added to pending and future civic digital legislation could tie these efforts together without displacing local priorities or constitutional lines.

I. A nation under civic digital stress

The best way to see the scale of the problem is not through abstract threat reports, but through public incidents that made civic dependence on digital systems suddenly visible.

In August 2019, more than 20 local governments in Texas were struck in a coordinated ransomware event, with the number of affected towns ultimately revised to 22. The attack did not require breaching twenty-two governments one by one. State and industry reporting indicated that the incident moved through a managed service provider environment and remote administration tooling, turning one shared digital dependency into a statewide civic failure point. Texas activated its State Operations Center, dispatched teams to affected sites, and restored business-critical services on an emergency basis within a week. The lesson was not merely that ransomware is dangerous. It was that shared digital intermediaries can convert local government into a tightly coupled system without public awareness that such coupling even exists.

A year later, Vermont offered a different but equally painful lesson. In October 2020, the University of Vermont Medical Center shut down internet access and its Epic electronic health record system after a ransomware attack crippled operations. The disruption delayed some chemotherapy and radiation treatments, slowed scans, postponed appointments, and forced some patients to seek care elsewhere. Twelve days into the outage, the hospital had only regained limited access to appointment schedules and chemotherapy plans, and hundreds of workers were reassigned or furloughed because core digital

systems were still down. A cyber incident had become a crisis in care delivery, labor allocation, and regional medical trust.

The same pattern resurfaced in Wyoming. In September 2019, Campbell County Health in Gillette was hit by ransomware that disabled roughly 1500 computers and forced the system to unplug machines to stop the spread. Emergency patients were diverted to other communities, surgeries and exams were canceled, and staff fell back on paper records while federal and state authorities investigated. Here again, the civic harm was not reducible to "IT downtime." It meant redirected ambulances, disrupted care, delayed procedures, and the practical weakening of a regional institution on which thousands depend.

In August 2024, the Port of Seattle and Seattle-Tacoma International Airport revealed the same structural vulnerability in transportation form. The cyberattack, later attributed to the Rhysida ransomware group, disrupted airport Wi-Fi, baggage systems, check-in kiosks, passenger displays, parking functions, and the Port's public web services. Staff had to use manual workarounds while systems were restored over time, and the Port later confirmed that about 90,000 people were affected by data theft tied to the incident. This was not simply a story about one airport having a bad week. It was a demonstration that heavily automated public infrastructure can fail in ways that are immediately visible to travelers while remaining structurally opaque to the public that funds and relies upon it.

These incidents are different in sector, geography, and political setting. Yet they rhyme. In one state, the chokepoint is a managed service provider; in another, an electronic health record platform; in another, a regional hospital network; in another, a port and airport system layered with digital dependencies. The common denominator is not simply "cybersecurity." It is civic digital stress: a condition in which public institutions have become deeply dependent on software, vendors, integrations, and automated platforms that citizens rarely see until failure turns them visible.

That phrase matters because it points to the gap in current debate. Americans are repeatedly shown the moment of breakdown - the diverted ambulance, the hand-written boarding pass, the delayed chemotherapy treatment, the frozen courthouse terminal - but not the cumulative pattern by which public systems became fragile in the first place. Breach notices, emergency press conferences, and forensic investigations tell the public that something has happened. They do not create continuous civic visibility into where risk is accumulating.

II. A reactive and mixed legislative response

States deserve more credit than they often receive. They are not waiting passively for Washington, nor are they uniformly asleep at the switch. The legislative and administrative response now visible across the country is substantial, if uneven.

Texas is a useful example because the 2019 multi-city ransomware event quickly pushed questions of governance, mutual aid, oversight, and local capacity into view. The state response emphasized operational recovery, but the episode also sharpened attention on managed service providers, remote-access tools, authentication, and the need for stronger local resilience standards. In other states, the emphasis has landed elsewhere.

Wyoming in 2023 created a Cybersecurity Division within the Department of Enterprise Technology Services and required public entities to establish authorized-use and cybersecurity policies. That move suggests a state trying to institutionalize baseline cyber governance rather than rely on ad hoc recovery alone. Washington's response to the Port of Seattle incident has unfolded through public notification, system restoration, and a broader policy conversation about critical infrastructure, legacy systems, and the validation of automated applications and dependencies. Vermont's experience has reinforced arguments for stronger hospital continuity planning, including offline procedures that can sustain care during prolonged network outages.

This legislative landscape is real, but it is mixed in several senses:

- First, it is reactive. Most bills and reforms emerge after a visible shock: a hospital outage, a municipal ransomware campaign, a court modernization failure, a port disruption, a benefits leak. The tempo is set by injury.

- Second, it is sector-specific. One state focuses on hospitals, another on MSPs, another on ports, another on local governments, another on AI systems or public records.

- Third, it is conceptually incomplete. Many proposals try to harden systems, fund response teams, centralize services, or regulate vendors, but few directly address the public's ongoing inability to see how civic digital risk is distributed across the institutions it depends upon.

That incompleteness is addressed. The Rider is not a rival to cybersecurity. It is not a substitute for segmentation, incident response, vendor assessment, continuity planning, or encryption. It is the connective tissue that can make those efforts legible across domains:

- If attached to a hospital continuity bill, the Rider could require privacy-respecting summaries of downtime preparedness, incident classes, and the duration for which facilities can safely operate when records systems fail.

- If attached to a local-government cyber resilience act, it could require anonymized reporting on backups, segmentation, restoration testing, and recurring points of municipal fragility that do not disclose exploitable detail.

- If attached to airport or port legislation, it could require high-level mapping of critical dependencies between baggage, check-in, display, parking, and communications systems, together with incident summaries and remediation progress that citizens can understand.

- If attached to state cyber-governance bills like Wyoming's, it could ensure that new divisions and policies generate a public-facing visibility layer rather than only internal compliance artifacts.

The word “non-agentic” (non-automating) is essential here. The Rider does not authorize a system to govern, recommend, decide, or act. It does not replace legislatures, courts, boards, or executive officers. It preserves meaningful human decision-making and constitutional authority. Its job is narrower and more Franklinian: to establish a common route by which knowledge of civic digital risk can move across institutions and into public deliberation.

That is why the postal analogy is useful. When Benjamin Franklin created what would become the U.S. Post Office in 1775, he did not attempt to abolish local differences in the colonies. He created an interoperable civic infrastructure through which separate places could communicate reliably enough to become part of a common public world. The contemporary states do not need a uniform digital code in every respect. They do need a standardized way for public digital stress to become visible in forms that legislators, auditors, journalists, and citizens can actually use.

At present, the country has the opposite condition. Every state now has a file of civic digital harms. Every state is improvising some combination of cyber response, modernization, procurement reform, continuity planning, or statutory adjustment. But the harms remain narratively scattered and the reforms remain legislatively disjointed. One state learns about rural hospital fragility, another about MSP concentration, another about airport automation, another about court portals, another about tax systems or housing platforms - and each responds as though the lesson were local rather than federal in the older, small-f sense of shared state experience.

A standardized rider would not solve ransomware. It would not end vendor failure, eliminate legacy systems, or make fragile institutions wealthy. But it would give states a common constitutional grammar for attaching public visibility to digital governance wherever it appears. That is a modest ambition, and precisely because it is modest, it is actionable.

The United States is no longer waiting to discover whether civic digital harm is real. It has already answered that question - fifty times over. The more urgent question is whether the states will continue to address those harms as isolated episodes, or whether they will begin to tie their responses together through a shared visibility standard.

Franklin built shared routes that allowed information to travel reliably between communities. Today’s challenge is to build civic visibility that allows digital risk to travel into democratic understanding before it becomes democratic crisis. This proposed cross-state legislative rider is a practical option for addressing escalating civic digital attacks in a more cooperative manner, while also respecting each state’s sovereignty.

The postal routes Franklin helped build did not appear by accident; they were designed, tested, and then quietly standardized by people who could see beyond a single town’s needs. Today’s ***Cross-State Civic Digital Visibility Rider*** would not spread by accident either. It would require editors, researchers, and public-interest technologists to bring this idea to the people who write and refine state law.

If this proposal resonates with you as a writer, policy staffer, civic advocate, or citizen, consider one small step: share it with organizations that already help states coordinate, such as the National Conference of State Legislatures, the Council of State Governments, or the National Association of State Chief Information Officers.

A single, standardized rider cannot solve civic digital stress on its own. But it can give these existing networks a practical tool for tying scattered state efforts into a more coherent, visible, and democratic response.

If the rider described above is adopted, the following questions may help to begin informed democratic reflection.

Addendum:

AFTER CROSS-STATE CIVIC DIGITAL VISIBILITY RIDERS ADOPTED: QUESTIONS for DEMOCRATIC DELIBERATION

This brief addendum is intentionally modest. It assumes that two or more states have already adopted a ***Cross-State Civic Digital Visibility Rider*** and now wish to consider what kinds of democratic questions may naturally follow from improved public visibility into civic digital dependencies, incidents, and recurring vulnerabilities.

It does not prescribe procurement policy, software architecture, vendor selection, interoperability mandates, or modernization blueprints. Its purpose is narrower: to encourage thoughtful democratic inquiry by helping legislators, executive officials, CIOs, auditors, journalists, and citizens ask better questions once the civic digital field has become more visible.

Constitutional Scope

The ***Rider*** belongs to the category of constitutional visibility standards rather than technology standards. Technology standards ask how software should be built; the ***Rider*** asks what democratic institutions should always be able to see about material digital risk while preserving meaningful human decision-making and prohibiting automated governmental authority.

For that reason, the questions below should be understood as invitations to democratic deliberation rather than as recommendations or instructions. Each state retains complete authority to answer them in its own constitutional, fiscal, administrative, and political manner.

Guiding Principle

The ***Rider*** embodies a simple sequence: visibility, understanding, deliberation, and democratic choice. It does not presume that improved visibility should automatically lead to standardized or predetermined reforms; rather, it enlarges the space for informed democratic judgment.

Improved visibility should enlarge democratic judgment, not replace it. Its purpose is to illuminate problems that elected institutions and the public may then consider through ordinary constitutional means.

Questions About Concentrated Dependence:

- Where do visibility reports suggest that multiple public entities rely on the same vendor, managed service provider, software platform, or remote administration pathway?

- Which shared digital intermediaries appear to create single points of failure across hospitals, courts, schools, ports, counties, or municipalities?

- Are there sectors in which concentration risk is not being adequately discussed because the underlying dependency only becomes visible during failure?

Questions About Continuity:

- When critical systems fail, which public functions can continue safely on paper, offline, or through manual workarounds, and for how long?

- Do visibility reports reveal recurring weaknesses in restoration testing, backup integrity, staffing resilience, or cross-agency coordination?

- Which institutions appear most vulnerable to prolonged disruption: health systems, courts, transportation hubs, tax agencies, schools, or local governments?

Questions About Interoperability:

- Where do public entities appear unable to share data, status information, or incident context because their systems are siloed or poorly integrated?

- Would better-documented interfaces, shared schemas, or common reporting formats improve resilience without requiring states to surrender policy control?

- Are there domains in which fragmentation itself has become a civic risk rather than merely an administrative inconvenience?

Questions About Procurement And Stewardship:

Improved visibility may naturally prompt questions about whether existing procurement and stewardship practices adequately support long-term democratic oversight.

- Do current contracts give public institutions adequate access to logs, incident records, audit trails, and system-dependency information needed for democratic oversight?

- Are vendors being asked to support exportable, machine-readable reporting that can sustain transparency over time?

- Where might long-term maintainability, accessibility, or transparency deserve greater weight in public procurement decisions?

Questions About Public Understanding, Accessibility, And Legibility:

- When systems degrade or fail, which residents are least able to navigate the disruption, including citizens with disabilities or limited digital access?

- Do public-facing summaries make civic digital risk understandable to ordinary citizens, or only to technical specialists?

- Which forms of reporting or visualization help the public grasp civic digital stress without requiring technical expertise?

- How should uncertainty be communicated honestly when visibility improves but definitive answers remain unavailable?

Questions About Democratic Deliberation:

- Once civic digital conditions become more visible, which questions should remain matters of elected legislative judgment rather than technical administration?

- Which forms of public reporting best strengthen democratic oversight without overwhelming citizens with unnecessary technical detail?

- Are legislatures receiving information that supports independent constitutional judgment rather than subtly steering policy conclusions?

- Does increased visibility broaden democratic participation, or merely improve technical administration?

- How can improved visibility strengthen public trust without encouraging the mistaken belief that technical clarity eliminates the need for democratic disagreement?

Questions About Institutional Learning:

- Are states learning from one another's visibility reports, or still treating each major disruption as an isolated local episode?

- The National Conference of State Legislatures, the Council of State Governments, and the National Association of State Chief Information Officers are well positioned to lead here. Could they help states compare visibility patterns without imposing one-size-fits-all solutions?

- What kinds of shared civic vocabulary might help separate visibility from automation, and deliberation from delegation?

Franklin's Continuing Lesson

Benjamin Franklin’s new postal service did not seek to standardize communities; he simply helped to create common routes through which communities could communicate more reliably. In the same spirit, cross-state visibility riders need not standardize how states build every digital system; they help standardize what democratic institutions are able to see about civic digital risk before crisis makes that risk unmistakable.

Visibility strengthens communication. Communication strengthens democratic deliberation. Democratic deliberation strengthens constitutional self-government.

Democratic Humility

The purpose of improved visibility is not to reduce democratic disagreement, but to ensure that disagreement is informed by a clearer understanding of shared civic conditions. Citizens and their representatives may continue to reach different conclusions about policy, and the ***Cross-State Civic Digital Visibility Rider*** simply seeks to ensure that those conclusions are formed in the light rather than in the dark.

Closing Reflection

The questions gathered here are intentionally open-ended. They are offered in the belief that better civic visibility should enlarge democratic judgment rather than replace it, and that states are more likely to cooperate around questions they remain free to answer for themselves than around prescriptions delivered from above.

Accordingly, this addendum should be understood not as a blueprint for modernization, but as an invitation to continued cross-state learning. As visibility improves, each state may discover different priorities, constraints, and solutions; that diversity is not a weakness of the rider, but one of its constitutional assumptions.